UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/462,616	04/03/2000	GUNTER MARINGER	0745/61002/N	5313

7590 05/20/2005

NORMAN H ZIVIN
COOPER & DUNHAM
1185 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/462,616	MARINGER ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 01/26/05. Applicant added claim 15. The amendment filed on 01/26/05 have been entered and made of record. Therefore, presently pending claims are 1-15.

Response to Arguments

Applicant's arguments filed 01/26/05 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that the present invention messages are exchanged between only two entities, the terminal and the network. This is not found persuasive. The limitations of claim 1 and claim 15 do not disclose message exchange between only two entities. The limitations disclose messages that are exchanged between the network, terminal, and network. The definition of network is a group of computers and associated devices. Therefore in the claims 1 and 15 the limitations include more that two entities by message exchange with a network.

Applicant argued further that Ganesan fails to disclose that response 1 sent from the terminal to the network is equal to challenge2, whereby the network has requested response 2 together with challenge 1 and response 1. Kc,s (Challenge 2) which must be calculated from message 4 where the knowledge of Kc,s allows the Response 2 (message 6) to be sent just as knowledge of Challenge 2 allows a correct Response 2. There message 6 includes Kc,s (Challenge 2), the Response 2 is the encrypted ts using Kc,s, by using Kc,s indicates that the

client knows Ks and therefore correct encryption of ts using Kc,s is equivalent to sending the value and therefore the Response 1.

Applicant argued further that Ganesan relates to a method for securing communications using split private key asymmetric cryptography, and does not disclose or suggest a method for mutual authentication of components in a communication network using a challenge-response method. The applicant has misrepresented the reference Ganesan, which is a method of authentication (abstract). Although the applicant has disclosed a method for mutual authentication of components in a network using a challenge-response method in the preamble, the applicant does not disclose the recited information in the body of the claim. In response to applicant's arguments, the recitation a method for mutual authentication of components in a network using a challenge-response method has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

The applicant argues further that Ganesan does not disclose a direct link between the service server and either of the authentication server or the ticket-granting server. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., direct link between the service server and either of the authentication server of the ticket granting server) are not recited in the rejected

claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claims recite sending responses and receiving requests from the network; a network is computers connected to each other. The computers in Ganesan are connected to each other as shown in Fig. 2.

The applicant argued further Schneier discloses only that keys may be random-bit strings generated by some automatic process, and does not disclose the authentication procedure of the present application as described above. This is not found persuasive. In the combination of Ganesan and Schneier, Ganesan discloses the authentication step and Schneier discloses the keys as random numbers.

The applicant argued further that Tsubakiyama does not indicate that the network interprets the message C1 as the message C2. This is not persuasive. The definition of interpret is to present in understandable terms. C1 is presented to the user named I in terms that the user can understand the value d1 and therefore use the combiner (11) to determine C2. Therefore the system interprets (places in understandable terms) the C1 as the message C2.

The applicant discloses the Clark et al does not disclose or suggest the use of two challenge values and two response values for authentication. The examiner regrets the typo that left Clark in the rejections for the dependent claims. This has been replaced by Ganesan to disclose the authentication process and Shneier for the keys as random numbers. Ganesan has been discussed above.

The examiner asserts that Ganesan and Schneier do teach or suggest the subject matter broadly recited in independent Claims 1 and 15. Dependent Claims 2-14 are also rejected at least

by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1-14 are respectfully maintained. Included in the rejection to claim 1 is the rejection for claim 15.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over the article by Ganesan (5,535,276) in view of Schneier.

Ganesan discloses a method for mutual authentication of components in a network using a challenge-response method to authenticate a client 110 to a server 150 (Fig. 2)

Requesting at least one data pair including a first random number (Challenge 1) and a first response (Response 1) from an authentication center using a request form the network. Ganesan discloses a client request that requests authentication services and therefore a data pair from a secure environment and specifically from an Authentication server (message 1 column 15 lines 33-60). After authenticating itself to the authentication server, and therefore to the secure environment as part of the request for authentication, the ticket granting server that is a part of the secure environment responds with the information (data pair) that the client uses to authenticate themselves

Regarding passing the first random number (Challenge 1) to the terminal which calculates the first response (Response 1) based upon an internally stored key and the first random number (Challenge 1). The Ticket granting server, that is a part of security environment (authentication center), sends message 4 to the client for communication. The message is encrypted by keys $K_{c,tgs}$ and K_s, which are random numbers resulting in a random number for the message. The internally stored key is Kc,tgs that the client uses to calculate the session key $K_{c,s}$ (column 17 lines 5-20).

Ganesan further discloses sending the calculated first response to the network. The response (message 5`) includes, among other parts, the session key $K_{c,s}$, which is used as part of the Challenge to the server 150. The message 5 is sent to the network (column 15 lines 10-16) and specifically to the server 150

Ganesan teaches responding to a second random number with a second response (Response 2) calculated in the authentication center, the response performed by the network wherein the first response sent from the terminal to the network is also used as the second random number (Challenge 2), whereby the network has previously requested the second response (Response 2) from the authentication. The second response (message 6`) contains the ticket information, which is calculated by the secure environment (column 5 lines 50-55 in combination with column 18 lines 1-10). The second random number is Ks, therefore the server 150 must prove its knowledge of Ks by sending the message 6 (Response 2). By proving the knowledge of Ks, then the network interprets the calculated first response sent back from the terminal as the Challenge 2. Since knowledge of Ks provides the correct message 6.

Ganesan does not expressly disclose the keys are random number.

However, Schneier discloses that good keys are random numbers (page 173).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art disclose keys as random number as in Schneier in the system of Ganesan. One of ordinary skill in the art would have been motivated to do this because random numbers make good keys; good keys are those that are not easily determined.

Claims 2-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan and Schneier as applied to claim 1 above, and further in view of Tsubakiyama (5,544,245).

In reference to claims 2 and 7, Ganesan does not expressly disclose a method wherein the network interprets the calculated first response sent back from the terminal as the second random number.

Tsubakiyama suggests a method (Fig. 2) where the message sent from the network N (C1) is used as a challenge to the user named i who interprets the challenge and responds to the challenge with the response C2. Therefore, the challenge is a message, which is interpreted and a response to the challenge is created and sent.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the response given by the terminal in the system of Ganesan as the challenge as in the method of Tsubakiyama. One of ordinary skill in the art would have been motivated to do this because it would provide a mutual authentication which enables the network and each user to authenticate each other without inviting the chosen plaintext attack and the known plaintext attack on the encryption algorithm in the authentication protocol and permits the deliver of a key for cipher communication without the need of increasing the amount of data to

be transmitted for the protocol for mutual authentication between the network and each user (Tsubakiyama column 2 lines 36-46).

In reference to claim 3, wherein the first random number (Challenge 1) and the second response (Response 2) are transmitted from the network (N) to the terminal (M) immediately successively in time (Tsubakiyama Fig. 2).

In reference to claim 4, wherein the data pair (Challenge 1/Response 2) is transmitted from the network (N) to the terminal (M) simultaneously, in the form of a single data set.

Ganesan does not expressly disclose sending the Challenge 1 and Response 2 in one transmission over the network.

However, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send the Challenge 1 and Response 2 in one transmission over the network if device has the technical capabilities. One of ordinary skill in the art would have been motivated to do this because consolidating the messages would reduce the traffic on the network.

In reference to claims 5 and 6, wherein the network requests data sets from the authentication center (AUC) in the form of triplet data sets (Challenge 1/Response 1/Response 2). Message 2 of section 6.3.1 discloses a system where the Challenge and response is sent to principal A.

In reference to claims 8-10, wherein the filling out process is carried out on a subscriber-specific basis, and wherein the complete length of the first response (Response 1) is shortened before transmission to the other station. Tsubakiyama discloses the manipulation of the data sent to the subscriber (user) to create a key (column 5 lines 12-15).

In reference to claim 11, wherein the network is a GSM network. Tsubakiyama discloses the network in Fig. 2. The GSM is a type of wireless network and therefore is encompassed in Tsubakiyama's description.

In reference to claim 12, wherein the network is a wire-based network. Tsubakiyama discloses a network in Fig. 2 which encompasses the wire-based network.

In reference to claim 13, wherein the individual, mutually authenticating components in a wire-based network are different monitoring units of computers which authenticate themselves with a central computer. The user in Tsubakiyama authenticates themselves to the network, which has a database of keys to use for communication with the different user. It therefore behaves like a central computer.

In reference to claim 14, wherein the AUC calculates the triplet data sets requested by the network and transmits these to the network off-line and independently of time, on request by the network, but in any case before the data interchange between the network and the terminal. Ganesan discloses the messages 1-4 (Fig. 2) being used for receiving and requesting the authentication data. Therefore, this is performed before the communications between the client 110 and the server 150.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, May 16, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100